WILSON THEOREMS FOR DOUBLE-, HYPER-, SUB- AND SUPER-FACTORIALS

CHRISTIAN AEBI AND GRANT CAIRNS

Abstract. We present generalisations of Wilson's theorem for double factorials, hyperfactorials, subfactorials and superfactorials.

1. Introduction

Wilson's theorem states that $(p-1)! \equiv -1$ if p is prime, and $(p-1)! \equiv 0$ otherwise, except for the one special case, $p = 4$. The result is attributed to John Wilson, a student of Waring, but it has apparently been known for over a thousand years; see [21], [8, Ch. II], [19, Ch. 11], [10, Chap. 3] and [24, Chap. 3.5]. The first proof was given by Lagrange [16]. We give generalisations of Wilson's theorem for the four standard generalisations of the factorial function.

Definition 1. For a natural number n,

(a) the *double factorial* $n!!$ is the product of the natural numbers less than or equal to n that have the same parity as n,
(b) the *hyperfactorial* $\mathrm{H}(n)$ is the number $\mathrm{H}(n) = \prod_{k=1}^{n} k^k$,
(c) the *subfactorial* $!n$ is the number of permutations of the set $\{1, 2, \ldots, n\}$ that fix no element,
(d) the *superfactorial* $\mathrm{sf}(n)$ is the number $\mathrm{sf}(n) = \prod_{k=1}^{n} k!$

The idea underlying our approach is the following: if there are sensible versions of Wilson's Theorem for these functions, then the numbers involved must be very special. If p is prime, then the obvious *special* numbers in the field $\mathbb{Z}_p$ are $0, \pm 1$ and when p is congruent to 1 mod 4, the two square roots of -1. So the task is to verify that these are the values taken, and determine which value is taken in each case. We find that this simple approach for prime p works surprisingly well. For composite numbers, the hyperfactorial, subfactorial and superfactorial functions are all easily treated, while the double factorial holds some unexpected interesting surprises. We present the results for double factorials in Theorems 3, 4, 6 and 7. The results for the superfactorial, hyperfactorial and subfactorial are given in Theorems 2, 5 and 8 respectively. The following result is an unexpected consequence of this study.

Theorem 1. *If p is an odd prime, then modulo p*

$$(p-1)!! \equiv \mathrm{sf}(p-1) \equiv (-1)^{\frac{p-1}{2}}\,\mathrm{H}(p-1).$$

2. Factorials: double, hyper, sub and super

According to the MacTutor History of Mathematics archive, the name *factorial* and the notation $n!$ were introduced by the French mathematician Christian Kramp in 1808 [15], but the symbol was not immediately universally adopted. In the English speaking world, the notation $\lfloor\underline{\mathrm{n}}$ was still commonly used at the end of the 19^{th} Century [5]. De Morgan wrote "Among the worst of barbarisms[1] is that of introducing symbols which are quite new in mathematical, but perfectly understood in common, language. Writers have borrowed from the Germans the abbreviation $n!$ to signify $1.2.3\ldots(n-1).n$, which gives their pages the appearance of expressing surprise and admiration that $2, 3, 4$, *&c.* should be found in mathematical results" [9].

Rev. W. Allen Whitworth[2] apparently didn't share De Morgan's view. Whitworth introduced the *subfactorial* and a symbol for it, in a paper that begins with the words: "A new symbol in algebra is only half a benefit unless it has a new name. We believe that the symbol $\lfloor\underline{\mathrm{n}}$ as an abbreviation of the continued product of the first n integers, was long in use before the name *factorial* n was adopted. But until it received its name it appealed only to the eye and not to the ear, and in reading aloud could only be described by a periphrasis" [25]. Subfactorial n is the number of permutations of the set $\{1, 2, \ldots, n\}$ that fix no element. There are many symbols for the subfactorial. Whitworth used the symbol $\lfloor\underline{\underline{\mathrm{n}}}$, in keeping with the notation for the factorial at the

[1] At some point, the word barbarisms was misspelt as barabarisms when quoted and this error has been reproduced in a great number of places.

[2] There is an amusing Australian connection concerning Whitworth. In the Cairns Post, 22 November 1890, an article reads: "The Rev. W. Allen Whitworth, in attempting a definition of gambling, as separable from mercantile speculation and legitimate enterprise, committed himself to the proposition that under ordinary circumstances and within the limits of moderation, it is (1) justifiable to back one's skill, (2) foolish to back one's luck, (3) immoral or fraudulent to back one's knowledge. There is no rule (4), but had there been it would doubtless have read – highly commendable to back Carbine". Carbine was the horse that won the Melbourne Cup in 1890.

time. These days $n¡$ is sometimes used, but $!n$ seems more common. De Morgan would not be happy!

The subfactorial has the following explicit formula.

$$!n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}. \tag{1}$$

The hyperfactorial function was also introduced in the 19^{th} Century [11, 14] and the superfactorial function followed at the turn of the Century [3], although the terms were introduced much later [23, 13].

Study of the double factorial goes back at least as far as 1948 [17], but it is probably much older. For even n, one has

$$n!! = 2^{\frac{n}{2}} \cdot \tfrac{n}{2}! \tag{2}$$

For n odd, $n!!$ coincides with the Gauss factorial $n_2!$, where in general $n_m!$ is the product of the natural numbers $i \leq n$ that are relatively prime to m [7]. For a recent paper on the properties of double factorials and their applications, see [12].

3. Motivation

Our motivation for considering the various factorial functions concerns the matrix

$$A = \begin{pmatrix} 1 & 2 & 3 & \dots & p-1 \\ 1 & 2^2 & 3^2 & \dots & (p-1)^2 \\ 1 & 2^3 & 3^3 & \dots & (p-1)^3 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 2^{p-1} & 3^{p-1} & \dots & (p-1)^{p-1} \end{pmatrix}.$$

There are many interesting facts and open questions related to the properties of the matrix A modulo p. For example, *Giuga's conjecture* is that the sum of the entries in the bottom row is congruent to -1 if and only if p is prime [4].

Proposition 1. *The above matrix A has determinant* $\mathrm{sf}(p-1)$*.*

Proof. Using the formula for the Vandermonde determinant [20, Chap. 1.2] we have

$$\begin{aligned}\det(A) &= (p-1)!\ \det\begin{pmatrix}1 & 1 & 1 & \dots & 1\\ 1 & 2 & 3 & \dots & p-1\\ 1 & 2^2 & 3^2 & \dots & (p-1)^2\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & 2^{p-2} & 3^{p-2} & \dots & (p-1)^{p-2}\end{pmatrix}\\ &= (p-1)! \prod_{1\le i<j\le p-1}(j-i)\\ &= (p-1)! \prod_{2\le j\le p-1}(j-1)! = \mathrm{sf}(p-1).\end{aligned}$$

□

Remark 1. Notice that $\mathrm{H}(p-1)$ is precisely the product of the elements on the main diagonal of A. We will return to the matrix A briefly in Section 5.

4. The connection between the superfactorial and the double factorial

Somewhat surprisingly, for prime p, the values $\mathrm{sf}(p-1)$ and $(p-1)!!$ are congruent. Before proving this result, let us recall a well known fact which Lagrange proved in [16] (see [12, 1]). Let p be an odd prime. Then

$$\left(\tfrac{p-1}{2}!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \tag{3}$$

Indeed, modulo p, one has $p-i \equiv -i$ for all i and so $(p-1)! \equiv (-1)^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}!\right)^2$ and the required claim follows from Wilson's Theorem.

Theorem 2. *If p is prime, then* $\mathrm{sf}(p-1) \equiv (p-1)!! \pmod{p}$.

Proof. The theorem is obvious for $p = 2$. In the following proof, p is odd and the congruences are taken modulo p. We have

$$\begin{aligned}\mathrm{sf}(p-1) &= (p-1)!\,(p-2)!\,(p-3)!\,\dots\,3!\,2!\,1!\\ &= (p-1)!!\,\left((p-2)!\,(p-4)!\,\dots\,3!\,1!\right)^2.\end{aligned}\tag{4}$$

Note that for all $1 \le i \le p-1$,

$$(p-i)! = \frac{(p-1)!}{(p-1)(p-2)\dots(p-i+1)} \equiv \frac{-1}{(-1)(-2)\dots(-i+1)}.$$

Hence

$$(p-i)! \equiv \frac{(-1)^i}{(i-1)!}. \tag{5}$$

So if $\frac{p-1}{2}$ is even, the factorials in (4) cancel in pairs, giving $\mathrm{sf}(p-1) \equiv (p-1)!!$, as required. If $\frac{p-1}{2}$ is odd, cancellation of the factorials in (4) leaves the middle term, giving $\mathrm{sf}(p-1) \equiv (p-1)!! \left(\frac{p-1}{2}!\right)^2$ and hence $\mathrm{sf}(p-1) \equiv (p-1)!!$, by (3). □

Remark 2. In the above proof, the factorials in $\mathrm{sf}(p-1)$ can also be cancelled in pairs using (5), leaving only the middle one, and so

$$\mathrm{sf}(p-1) \equiv (-1)^{\sum_{i=1}^{\frac{p-1}{2}} i} \cdot \tfrac{p-1}{2}! = (-1)^{\frac{p^2-1}{8}} \cdot \tfrac{p-1}{2}! \tag{6}$$

Comparing this with $(p-1)!! = 2^{\frac{p-1}{2}} \cdot \frac{p-1}{2}!$, we obtain a simple derivation that $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}}$. In the following we will also require Euler's criterion [8, Ch. III]: 2 is a quadratic residue if and only if $2^{\frac{p-1}{2}} \equiv 1$. Using this and Legendre's symbol we get a basic property of Gaussian reciprocity which allows to write:

$$(p-1)!! \equiv \left(\frac{2}{p}\right) \cdot \frac{p-1}{2}! \equiv (-1)^{\frac{p^2-1}{8}} \cdot \frac{p-1}{2}! \pmod{p}. \tag{7}$$

5. The double factorial in the prime case

If p is an odd prime, then (3) and (7) give

$$((p-1)!!)^2 \equiv \left(\tfrac{p-1}{2}!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \tag{8}$$

In particular, $(p-1)!! \equiv \pm 1 \pmod{p}$ when $p \equiv 3 \pmod{4}$. The following result gives a more precise statement of this fact.

Theorem 3. *Suppose that p is an odd prime and $p \equiv 3 \pmod{4}$. Then $(p-1)!! \equiv (-1)^{\nu} \pmod{p}$, where ν denotes the number of nonquadratic residues j with $2 < j < \frac{p}{2}$.*

Proof. Once again, the congruences will be taken modulo p unless otherwise stated. Let $s := \frac{p-1}{2}$ and $\mathbb{Z}_p^+ := \{1, 2, \ldots, p-1\}$. To evaluate the factor $s!$ in (7) we use an argument that Mordell attributed to Dirichlet [18]. Consider the involution $\varphi : x \mapsto p-x$ on $\mathbb{Z}_p^+$. Since $p \equiv 3 \pmod{4}$, p cannot be expressed as a sum of two squares, and so φ interchanges the set QR of quadratic residues with the set NR of nonquadratic residues. Let $QR = \{r_1, r_2, \ldots, r_s\}$ and $NR = \{n_1, n_2, \ldots, n_s\}$, with elements listed in natural order. Then

$$s! = r_1 r_2 \ldots r_{s-N}\ n_1 n_2 \ldots n_N \equiv (-1)^N r_1 r_2 \ldots r_s,$$

where N denotes the number of nonquadratic residues $j < \frac{p}{2}$. As $p \equiv 3 \pmod{4}$, one has $r_1 r_2 \ldots r_s \equiv 1$; see [22, p. 75]. Hence $s! \equiv (-1)^N$. Thus by Remark 2, $(p-1)!! \equiv 1$ if and only if either 2 is quadratic residue and N is even, or 2 is nonquadratic residue and N is odd. Thus $(p-1)!! \equiv 1$ if and only if ν is even. □

When $p \equiv 1 \pmod 4$, we have $((p-1)!!)^2 \equiv -1 \pmod p$. In this case, because -1 is a quadratic residue, the involution φ used in the proof of Theorem 3 leaves the sets QR and NR invariant, so it is not useful. Instead we consider the involution $\psi : x \mapsto x^{-1}$ of $\mathbb{Z}_p^+$. It turns out that this approach is applicable for all odd primes.

Theorem 4. *Suppose that p is an odd prime. Let μ denote the number of elements j less than $\frac{p}{2}$ such that the inverse j^{-1} of j modulo p is also less than $\frac{p}{2}$.*

(a) *If $p \equiv 3 \pmod 4$, then $(p-1)!! \equiv (-1)^{\frac{\mu+1}{2}} \pmod p$.*
(b) *If $p \equiv 1 \pmod 4$, then $(p-1)!! \equiv (-1)^{\frac{\mu+1}{2}} i_p \pmod p$, where i_p is the unique natural number less than $\frac{p}{2}$ with $i_p^2 \equiv -1 \pmod p$.*

Proof. We use the same notation as in the proof of Theorem 3. Notice that if $j < \frac{p}{2}$ and $j^{-1} < \frac{p}{2}$, then the two terms cancel in $\frac{p-1}{2}!$. On the other hand, if $j < \frac{p}{2}$ and $j^{-1} > \frac{p}{2}$, then $p - j^{-1} < \frac{p}{2}$ and provided $j \neq p - j^{-1}$, the product $j.(p-j^{-1})$ in $\frac{p-1}{2}!$ gives -1.

If $p \equiv 3 \pmod 4$, the number -1 is not a quadratic residue and so there is no $j < \frac{p}{2}$ with $j = p - j^{-1}$. In this case, $b = \frac{p-1}{2}! \equiv (-1)^{\frac{s-\mu}{2}}$, where $s = \frac{p-1}{2}$. Hence $(p-1)!! = ab \equiv (-1)^{\frac{p^2-1}{8}+\frac{s-\mu}{2}}$. Let $p = 4k+3$. Then $\frac{p^2-1}{8} + \frac{s}{2} = 2k^2 + 4k + \frac{3}{2}$. Hence $(p-1)!! \equiv (-1)^{\frac{3-\mu}{2}} \equiv (-1)^{\frac{\mu+1}{2}}$, as required.

If $p \equiv 1 \pmod 4$, we argue in the same manner, but now i_p is the unique number with $i_p < \frac{p}{2}$ and $i_p = p - i_p^{-1}$. Hence $\frac{p-1}{2}! \equiv (-1)^w i_p$, where $w = \frac{s-\mu-1}{2}$. Thus $(p-1)!! = ab \equiv (-1)^{\frac{p^2-1}{8}+\frac{s-\mu-1}{2}} i_p$. Let $p = 4k+1$. Then $\frac{p^2-1}{8} + \frac{s}{2} = 2k^2 + 2k$. Hence $(p-1)!! \equiv (-1)^{\frac{\mu+1}{2}} i_p$, as required. □

Together Theorems 3 and 4 provide the following equivalence.

Corollary 1. *If p is an odd prime with $p \equiv 3 \pmod 4$, then the number ν, of nonquadratic residues i with $2 < i < \frac{p}{2}$, is even if and only if the number μ of elements j less than $\frac{p}{2}$ such that the inverse j^{-1} of j modulo p is also less than $\frac{p}{2}$, is congruent to 3 modulo 4.*

Remark 3. The results of Theorems 3 and 4 can be expressed in terms of class field numbers h, but the resulting statements are not as succinct as those given above. For the $p \equiv 3 \pmod 4$ case, one can use $h(-p) = 2N - 1 \pmod 4$; see [18]. For $p \equiv 1 \pmod 4$, the result can be expressed in terms of $h(p)$ and the fundamental unit of the associated real quadratic number field; see [6].

We can now give the connection between the hyperfactorial and double factorial.

Theorem 5. *For p an odd prime, the hyperfactorial and double factorial are connected by the relation* $\mathrm{H}(p-1) \equiv (-1)^{\frac{p-1}{2}}(p-1)!! \pmod{p}$.

Proof. Using Fermat's Little Theorem and Wilson's Theorem, we have

$$\begin{aligned}\mathrm{H}(p-1) = \prod_{k=1}^{p-1} k^k &= \frac{(\mathrm{sf}(p-1))^{p-1}}{\mathrm{sf}(p-2)} \\ &= \frac{(\mathrm{sf}(p-1))^{p-1}(p-1)!}{\mathrm{sf}(p-1)} \\ &\equiv \frac{-1}{\mathrm{sf}(p-1)} \equiv \frac{-1}{(p-1)!!},\end{aligned}$$

by Theorem 2. By (8), we have

$$((p-1)!!)^{-1} \equiv \begin{cases} (p-1)!! & : \text{ if } p \equiv 3 \pmod{4} \\ -(p-1)!! & : \text{ if } p \equiv 1 \pmod{4}. \end{cases}$$

Thus $\mathrm{H}(p-1) \equiv (-1)^{\frac{p-1}{2}}(p-1)!!$, as required. □

Remark 4. Note that by Proposition 1, Remark 1 and Theorems 2 and 5, modulo p the determinant of the matrix A of Section 3 is $(-1)^{\frac{p-1}{2}}$ times the product of the elements on the main diagonal of A.

6. Composite numbers

When n is composite and $n \neq 4$, one has $(n-1)! \equiv 0 \pmod{n}$. Similarly, it is obvious that $\mathrm{sf}(n-1) \equiv 0 \pmod{n}$ and $\mathrm{H}(n-1) \equiv 0 \pmod{n}$ for all composite natural numbers n. For the double factorial, the situation is more nuanced. The case of odd composites is not difficult.

Theorem 6. *If n is a composite odd natural number, then* $(n-1)!! \equiv 0 \pmod{n}$ *if $n > 9$, while* $8!! \equiv 6 \pmod{9}$.

Proof. Let n be a composite odd natural number. If $n = ab$, where a, b are co-prime, then $a, b < \frac{n-1}{2}$, so $\frac{n-1}{2}! \equiv 0 \pmod{n}$. So we may assume that n is of the form $n = p^k$ for some odd prime p, where $k \geq 2$. If $k > 2$, then p, p^{k-1} are distinct and $p, p^{k-1} < \frac{n-1}{2}$, so $\frac{n-1}{2}! \equiv 0 \pmod{n}$. If $n = p^2$ and $p > 3$, then $p, 2p$ are distinct and $p, 2p < \frac{n-1}{2}$, so once again $\frac{n-1}{2}! \equiv 0 \pmod{n}$. It remains to consider $n = 9$, which can be calculated by hand. □

However, when n is even, the pattern is less obvious.

Theorem 7. *Suppose that $n = 2^i(2k+1)$, where $i \geq 1$ and $k \geq 0$.*

(a) *if $i = 1$, then $(n-1)!! \equiv 2k+1 \pmod{n}$,*
(b) *if $i = 2$, then $(n-1)!! \equiv -(2k+1) \pmod{n}$,*
(c) *if $i > 2$, then $(n-1)!! \equiv (2k+1)^{2^{i-2}} \pmod{n}$.*

Proof. We first treat the case $k = 0$. Recall that for an arbitrary integer n, Gauss' generalisation of Wilson's Theorem [10, Chap. III] (see also [2]) states that if I denotes the set of invertible elements in $\mathbb{Z}_n$, then

$$\prod_{s\in I} s \equiv \begin{cases} -1 & : \text{ if } n = 4, p^\alpha, 2p^\alpha \ (p \text{ an odd prime}) \\ 1 & : \text{ otherwise} \end{cases} \pmod{n}.$$

For $n = 2^i$ the set of odd elements of $\mathbb{Z}_n$ is precisely the group of invertible elements in $\mathbb{Z}_n$. Hence Gauss' result gives

$$(n-1)!! \equiv \begin{cases} -1 & : \text{ if } i = 2 \\ 1 & : \text{ otherwise,} \end{cases} \pmod{n}.$$

as required.

Now assume $k > 0$. By the Chinese remainder theorem, the map

$$\begin{aligned} \varphi : \mathbb{Z}_n &\to \mathbb{Z}_{2^i} \times \mathbb{Z}_{2k+1} \\ m &\mapsto (\varphi_1(m), \varphi_2(m)) \end{aligned}$$

is a ring isomorphism, where $\varphi_1(m)$ (resp. $\varphi_2(m)$) is the reduction of m modulo 2^i (resp. $2k+1$). The inverse map is given by

$$\varphi^{-1}(x, y) \equiv by2^i + ax(2k+1) \pmod{n}.$$

where $a(2k+1) + b2^i = 1$. The numbers a and b are defined modulo n. The proof focuses on the value of a. For $i = 1$ we may take $a = 1$. For $i = 2$, we can take $a = (2k+1)$. For $i \geq 3$, note that as the set of odd elements of $\mathbb{Z}_{2^i}$ is the group of invertible elements in $\mathbb{Z}_{2^i}$, so by Euler's Theorem, $(2k+1)^{2^{i-2}} \equiv 1 \pmod{2^i}$. Thus we may take $a = (2k+1)^{2^{i-3}}$ when $i \geq 3$. We have

$$\varphi((n-1)!!) = \prod_{\substack{x\in\mathbb{Z}_{2^i},\ y\in\mathbb{Z}_{2k+1} \\ x \text{ odd}}} (x, y) = \left(\prod_{\substack{x\in\mathbb{Z}_{2^i} \\ x \text{ odd}}} x, \prod_{y\in\mathbb{Z}_{2k+1}} y \right) = \left((2^i-1)!!, 0\right).$$

Now from the $k = 0$ case treated above,

$$(2^i - 1)!! \equiv \begin{cases} -1 & : \text{ if } i = 2 \\ 1 & : \text{ otherwise.} \end{cases} \pmod{2^i}.$$

So when $i = 1$ we have

$$(n-1)!! = \varphi^{-1}(1,0) \equiv a(2k+1) = (2k+1).$$

When $i = 2$ we have

$$(n-1)!! = \varphi^{-1}(-1,0) \equiv -a(2k+1) = -(2k+1)^2.$$

Finally, for $i \geq 3$ we have

$$(n-1)!! = \varphi^{-1}(1,0) \equiv a(2k+1) = (2k+1)^{2^{i-2}}.$$

□

7. The subfactorial

For the (standard) factorial, the double factorial, the hyperfactorial and the superfactorial, the value at number n is congruent to zero mod n. It is in part for this reason that the value at $n-1$ is of interest mod n. For the subfactorial however, the situation is different. Here the natural generalisation of Wilson's Theorem is the following.

Theorem 8. *If n is a natural number, then $!n \equiv (-1)^n \pmod{n}$.*

Proof. Modulo n we have from (1)

$$!n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!} = (-1)^n + n! \sum_{i=0}^{n-1} \frac{(-1)^i}{i!} \equiv (-1)^n \pmod{n}.$$

□

References

1. Christian Aebi and Grant Cairns, *Catalan numbers, primes, and twin primes*, Elem. Math. **63** (2008), no. 4, 153–164.
2. ______, *A property of twin primes*, Integers **12** (2012), #A7.
3. E. W. Barnes, *The theory of the G-Function*, Quart. J. Pure Appl. Math **31** (1900), 264–314.
4. D. Borwein, J. M. Borwein, P. B. Borwein, and R. Girgensohn, *Giuga's conjecture on primality*, Amer. Math. Monthly **103** (1996), no. 1, 40–50.
5. Florian Cajori, *History of mathematical notations vol. 2*, The Open Court Publishing Company, 1929.
6. S. Chowla, *On the class number of real quadratic fields*, Proc. Nat. Acad. Sci. U.S.A. **47** (1961), 878.
7. John B. Cosgrave and Karl Dilcher, *An introduction to Gauss factorials*, Amer. Math. Monthly **118** (2011), no. 9, 812–829.

8. Harold Davenport, *The higher arithmetic : an introduction to the theory of numbers*, Hutchinson, London, 1952.
9. Augustus De Morgan, *Symbols and notation*, Penny Cyclopaedia Vol. 23, 1842, pp. 442 – 445.
10. Leonard Eugene Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality*, Chelsea Publishing Co., New York, 1966.
11. J.W.L. Glaisher, *On the product* $1^1 2^2 3^3 \dots n^n$, Messenger of Math. **7** (1877-78), 43–47.
12. Henry Gould and Jocelyn Quaintance, *Double fun with double factorials*, Math. Mag. **85** (2012), no. 3, 177–192.
13. Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994, A foundation for computer science.
14. Hermann Kinkelin, *Ueber eine mit der Gammafunction verwandte Transcendente und deren Anwendung auf die Integralrechnung*, J. Reine Angew. Math. **57** (1860), 122–138.
15. Christian Kramp, *Elémens d'arithmétique universelle*, Hansen, 1808.
16. J. L. Lagrange, *Démonstration d'un théorème nouveau concernant les nombres premiers*, Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin (1770), 123–133.
17. B. E. Meserve, *Classroom Notes: Double Factorials*, Amer. Math. Monthly **55** (1948), no. 7, 425–426.
18. L. J. Mordell, *The congruence* $(p-1/2)! \equiv \pm 1 \pmod{p}$, Amer. Math. Monthly **68** (1961), 145–146.
19. Oystein Ore, *Number Theory and Its History*, McGraw-Hill Book Company, Inc., New York, 1948.
20. V. V. Prasolov, *Problems and theorems in linear algebra*, Translations of Mathematical Monographs, vol. 134, American Mathematical Society, Providence, RI, 1994, Translated from the Russian manuscript by D. A. Leĭtes.
21. Roshdi Rashed, *Ibn al-Haytham et le théorème de Wilson*, Arch. Hist. Exact Sci. **22** (1980), no. 4, 305–321.
22. H. E. Rose, *A course in number theory*, second ed., Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1994.
23. N. J. A. Sloane, *A handbook of integer sequences*, Academic Press, New York-London, 1973.
24. John Stillwell, *Elements of number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003.
25. W. Allen Whitworth, *Sub-factorial N*, Messenger of Math. **7** (1877-78), 145–147.

Collège Calvin, Geneva, Switzerland 1211
E-mail address: christian.aebi@edu.ge.ch

Department of Mathematics and Statistics, La Trobe University, Melbourne, Australia 3086
E-mail address: G.Cairns@latrobe.edu.au